Information System Security Protection Based on SDN Technology in Cloud Computing Environment

Huichao Liang*, Han Liu, Fangfang Dang, Lijing Yan, Dingding Li
State Grid Henan Information & Telecommunication Company (Data Center), Zhengzhou, Henan 450000, China
894019143@qq.com
*Corresponding author

2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA) | 978-1-6654-3561-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/AEECA52519.2021.9574276

***Abstract*—Cloud computing is a modern computing mode based on network, which is widely participated by the public, and provides virtualized dynamic computing resources in the form of services. Cloud computing builds an effective communication platform with the help of computer internet, so that users can get the same computing resources even if they are in different areas. With its unique technical characteristics and advantages, cloud computing has been deployed to practical applications more and more, and the consequent security problems of cloud computing have become increasingly prominent. In addition to the original cloud computing environment, this paper proposes to build a secure cloud with cloud technology, deploy security agents in the business cloud, connect the business cloud, security cloud and security agents through SDN (software defined network) technology, and dynamically divide the business cloud into logically isolated business areas through security agents. Therefore, security is separated from the specific implementation technology and deployment scheme of business cloud, and an information security protection scheme under cloud computing environment is proposed according to the characteristics of various factors, so as to enhance the security of network information.**

Keywords—Cloud computing, Information security, SDN

I. INTRODUCTION

With the continuous promotion of Internet applications, more and more information and data are stored with the help of computers, and the cost of data storage is also higher and higher. It is urgent to build a new platform to solve the problems existing in the network development and user use, and the concept of cloud computing arises at the historic moment [1]. Cloud computing provides users with computing, storage and other capabilities in the form of resources. Users don't have to care where and how to provide resources, but use them on demand [2]. Through this way of intelligent allocation of computer resources, we can make full use of computer resources, thus reducing unnecessary waste and improving the overall work efficiency [3]. Because the cost of construction, use and maintenance of cloud computing is far lower than that of traditional solutions, it is welcomed by users, and related technologies and applications have been developing rapidly. Based on the way of resource virtualization, cloud computing uses the transmission capacity of high-speed Internet to centralize the distributed computing, storage, service components, network software and other resources on the network, and transfer the data processing process from personal computer or server to a large computing center [4]. Cloud computing is distributed on a large number of distributed computers instead of local computers or remote servers. The operation of enterprise data center will be more similar to that of Internet. This enables enterprises to switch resources to the applications they need, and access computers and storage systems according to their needs [5].

Cloud computing for the entire information field can be said to be a technological innovation, it uses the computer Internet to build an effective communication platform, even if users are in different regions, they can get the same computing resources [6]. Cloud computing belongs to a business computing model, which can easily and quickly dock with a specific business model, connect to the cloud computing server resource pool through the network, and flexibly allocate the size of the computer resource pool [7]. Cloud computing technology has diversified technical approaches and tolerant computing capabilities. When processing data, cloud computing technology with its own characteristics can quickly and accurately meet the requirements of users [8]. With its unique technical characteristics and advantages, cloud computing is more and more deployed to practical applications, followed by cloud computing security problems are increasingly prominent [9]. With the rapid development of the Internet, more and more information systems have been widely used, and the security of information systems has been paid unprecedented attention. After the construction of the information system is completed, it is in the operation and maintenance stage for a long time. Therefore, it is very necessary to do a good job in the security work of the operation and maintenance stage of the information system [10]. In addition to the original cloud computing environment, this paper proposes to build a security cloud with cloud technology, deploy security agents in the business cloud, connect the business cloud, security cloud and security agent through SDN (Software Defined Network) technology, and dynamically divide the business cloud into multiple business areas with logical isolation through security agents.

II. INFORMATION SECURITY RISK IN CLOUD COMPUTING ENVIRONMENT

With the rapid development of cloud computing, it is also facing great challenges of information security. At present, security has become the most important factor that puzzles the greater development of cloud computing. In the general network boundary protection, the boundary is divided according to the category and importance of resources, and the problem of fuzzy boundary will not occur in this modular environment. In the cloud computing server, due to the highly complex virtualization technology and control technology, as well as the high integration of a large number of devices, the traditional definition of network boundaries becomes more and more complex and difficult to determine. If the staff make mistakes or deliberately attack

Authorized licensed use limited to: Mukesh Patel School of Technology & Engineering. Downloaded on July 11,2023 at 05:51:40 UTC from IEEE Xplore. Restrictions apply.

during operation, it will bring internal risks. Workers are sometimes attacked maliciously by hackers in their work, which will bring external risks. In order to effectively improve the information security in the cloud computing environment, relevant departments should focus on the causes of human factors and design a cloud computing system that is people-oriented and meets the needs of users. SDN technology can record and schedule all the data flows to and through the nodes. Overlay network can make the user's data path become the only path, which will not be acquired or transferred from the outside, thus ensuring that the data will not be easily deceived or stolen during transmission [11].

The security of data storage depends on data access audit, access user authority control and data consistency verification. The network summary level system framework under the information ecology is shown in Figure 1.

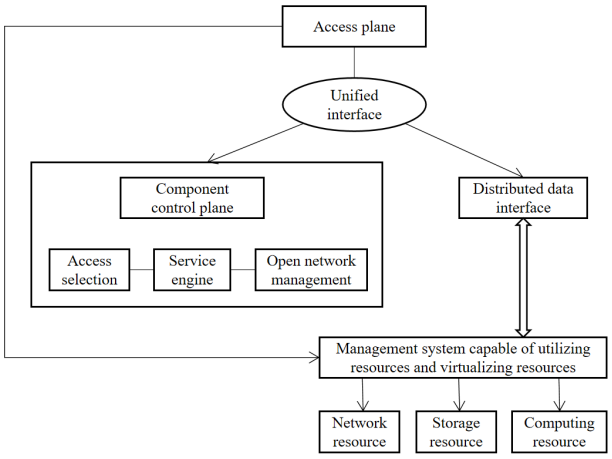

Figure 1 Network summary level system framework

Data encryption technology in server can use volume label storage encryption technology and object storage encryption technology. Object storage encryption technology is to achieve the purpose of defending against invasion by encrypting files to a certain extent. When users read data from the cloud server through the server, they must encrypt and decrypt the data through the encryption device, and then the data will be transmitted to the instance volume label and presented to the users. Large customer service is often different from public cloud services, private cloud services often have frequent virtual machine migration and other actions, while security deployment is often a customized service strategy made according to environmental changes. After the business model changes, security services often need to be re-formulated, and the intermediate time and link will cause cloud services of large customers to be exposed to security threats. According to the definition of cloud computing and the understanding of related concepts, the operation mode of cloud computing is to hand over user data and corresponding computing tasks to server networks and database systems running around the world, and the operations such as user data storage, user data processing and protection are all completed in the "cloud" [12]. In this way, the user's data is inevitably in an unsafe state that may be destroyed and stolen, and more and more detailed personal privacy information is exposed on the network.

Multi-tenant technology and virtualization technology play an extremely important role in the application of cloud computing. With the help of multi-tenant technology, different users can share applications and effectively reduce operating costs. With the help of virtualization technology, the storage host and other functions are virtualized, which effectively enhances the use efficiency of information resources. The hierarchical information security organization structure is shown in Figure 2.

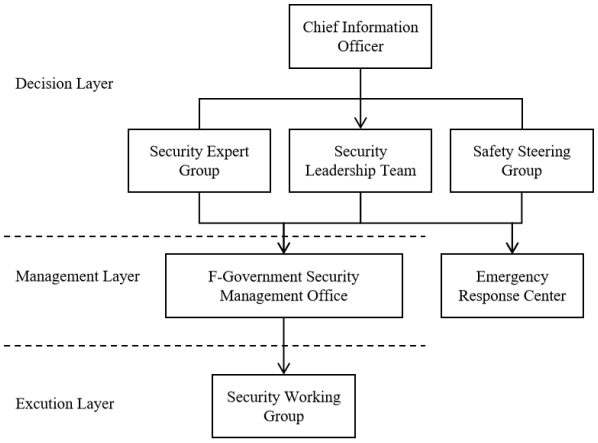

Figure 2 Hierarchical information security organization structure

Automatic migration of virtual machines in virtualized environment is one of the important features of cloud computing environment. In order to follow the migration of this virtual machine, the resource configuration of the business system itself and the access port attribute of this virtual machine are responding positively and providing adaptive means. Cloud computing security incidents occur frequently, and its stability, security and integrity are all problems to be solved. The establishment of information security protection system in cloud computing environment will surely make cloud computing develop healthily and orderly. Cloud computing technology will not be restricted by categories and regions when spreading files, and there will be no delay problem. Cloud communication makes the dissemination of information more convenient, makes all kinds of ideas spread to the society quickly, affects people's mentality, and changes some people's political ideas, which greatly weakens the ability of government departments to control information. The security of cloud hosts will directly affect the security of cloud data. In many cases, most of the cloud data leaks are due to loopholes in cloud servers or unreasonable configuration, resulting in being used by criminals. The storage of enterprise's core data in cloud computing environment can not be separated from the operation and audit of administrators. If there is any omission in the internal management of service providers, it may cause internal personnel to steal user data without permission, thus damaging the interests of users.

III. Research on Information Security Strategy Based on SDN Technology

A. Building information security system based on heterogeneous data

Under the cloud computing environment, each user's information security will be affected by different factors, which will bring certain security risks. Relevant departments must pay more attention to the security of data and information, establish a perfect information and data security system, user identity management system and information security protection system, and improve

Authorized licensed use limited to: Mukesh Patel School of Technology & Engineering. Downloaded on July 11,2023 at 05:51:40 UTC from IEEE Xplore. Restrictions apply.

information security as much as possible. In order to ensure the safety of data and avoid the random use of data, it is necessary to set the user's right to use data to ensure that the data is used within the allowed range under the condition of meeting certain safety requirements. In case of information system change, the person in charge of system change will make clear the user's requirements and form a requirement change document. After that, it will review and analyze the demand change document with the system operation and maintenance party and the security operation and maintenance party, determine the change content, and form the change plan document. The construction of information security protection system is based on certain data calling authority and specific data center as reference standard [13]. Only in this way can we ensure that the designed protection system can meet the requirements of authority in actual use and better ensure information security. Because most servers use Linux system as the server system, which is named after open source and practicality, one disadvantage of open source is that anyone can audit the system code, so there are more system vulnerabilities than closed source systems. At the same time, the repair speed will be faster than other operating systems.

Data packets output by traditional switch will be received by several SDN switches connected with it and forwarded according to SDN mode. Once there is no corresponding flow table in the SDN switch, the SDN switch uploads the packetin message to the SDN controller. The algorithm flow is shown in Figure 3.

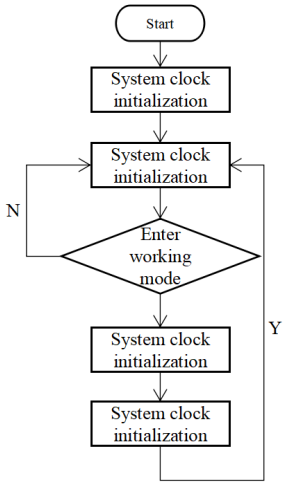

Figure 3 Algorithm flow

Suppose $\psi(x) \in L^2(R), L^2(R)$ is the square integrable function space, and the Fourier transform $\psi(\omega)$ satisfies the condition:

$$\int_R \left(\frac{|\psi(\omega)|^2}{\omega} \right) d\omega < \infty \tag{1}$$

The corresponding equivalent conditions are:

$$\int_{-\infty}^{+\infty} \psi(x) dx = 0 \tag{2}$$

Then $\psi(x)$ is called a basic wavelet or wavelet mother function, and the above formula is called the admissible condition of the wavelet function. The continuous wavelet basis function $\psi_{a,b}(x)$ expands and translates the wavelet mother function $\psi(x)$. Set its expansion factor to a, the translation factor to b, and the function after translation and expansion to be $\psi_{a,b}(x)$, then:

$$\psi_{a,b}(x) = a^{-\frac{1}{2}} \psi\left(\frac{(x-b)}{a} \right), a > 0, b \in R \tag{3}$$

Therefore, $\psi_{a,b}(x)$ is called the wavelet basis function that depends on the parameters a and b.

For the change implementation work, it is necessary to formulate a detailed change implementation plan, and the system change person in charge shall review the implementation plan together with the safety operation and maintenance party, and the system operation and maintenance party shall complete the change work according to the reviewed plan. For virus protection, it can be protected by installing antivirus software and firewall. At the same time, virtual network technology can be used for physical data isolation to maintain data security. No matter how to protect the server, it should not be done at the expense of the efficiency of the server. In the process of building an identity management system, it is necessary to deal with related privacy issues and complete the authentication of identity attributes, so as to better meet the specific requirements of different identity management systems and achieve the expected standards. In order to improve the security protection capability of the identity management system, it is necessary to fully and effectively combine the identity management system with other management systems involved in cloud computing to carry out research and development, so that the identity management system can run smoothly and play a role in protecting information security.

B. Operation management and control

Information system environment security protection focuses on using information guarantee technology to ensure the availability, integrity and confidentiality of user information when entering, leaving or residing in clients and servers. When constructing the identity management system, it is necessary to comprehensively analyze the contents of user management and information security. In actual operation, it is necessary to refer to the user's identity information and restrictions to realize the whole process of requesting users. At the same time, we should pay special attention to some privacy issues, handle them correctly, and complete the authentication of user identity attributes. For the security of data transmission inside the server, the most effective way to protect it is to realize the security of data through ciphertext transmission. In the traditional server data storage, the data will be stored in clear text. Once the server is invaded, the security of these data will be greatly threatened. Ciphertext transmission can further improve the security of information systems under cloud computing [14]. In fact, the development of cloud computing is based on the

Authorized licensed use limited to: Mukesh Patel School of Technology & Engineering. Downloaded on July 11,2023 at 05:51:40 UTC from IEEE Xplore. Restrictions apply.

development of Internet technology. To a great extent, the information security of cloud computing is directly affected by network security. In order to strengthen the protection of information security, it is necessary to speed up the development of current cloud computing technology. In practical work, we should be good at using privacy protection protocol to verify the identity attributes of users and build a new advanced identity management system.

The breakthrough of cloud computing can not be separated from the development of Internet technology, and the security level of the network will have a great impact on the information security in the cloud computing environment. In order to formulate comprehensive information security protection measures, it is necessary to innovate the cloud computing technology to make it more perfect. Figure 4 is a schematic diagram of the structure of intrusion detection system in cloud computing environment.

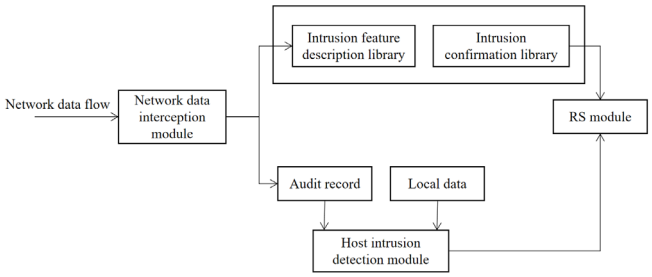

Figure 4 Schematic diagram of the structure of the intrusion detection system

In order to further enhance the security protection capability of the identity management system, we can also comprehensively consider the information security protection in the cloud computing related management system. In practical work, the relevant personnel should combine the data calling authority with the corresponding data center, so that the protection system can meet the requirements of various authorities in specific applications, thus ensuring the security of information. Therefore, the data center should be taken as a reference when establishing the security protection system. Cooperate on the basis of mutual benefit, build a unified management platform, connect different clouds to form a unified whole, and ensure that the information of all parties can be circulated and integrated more quickly and effectively in the platform, so as to better support the play of cloud services [15]. Staff should reasonably set the access rights of data users, so as to prevent the random use of data, ensure that the data is used within the safety standards and specifications, and thus improve the data security.

IV. Conclusions

The emergence of cloud computing technology has brought great convenience to users, allowing users to get the same computing resources at any time without being restricted by regions, and the running cost is relatively low. With the continuous application of cloud computing in all aspects of people's lives, its system security is becoming more and more important. Security is the premise of any operation for both cloud server manufacturers and users. Security has become the most important factor that puzzles the greater development of cloud computing. To some extent, whether and how to solve the security problems of cloud computing will directly determine the future development trend of cloud computing.

In the cloud computing environment, each cloud computing user's information security is affected by various factors to varying degrees, and there are security problems. It is necessary to build an information data security system and a corresponding user identity management system based on the research on data security. In the era of cloud computing, the explosive growth of data and the ever-changing applications bring new challenges to network security protection. Therefore, the construction of cloud security protection system is an important direction of development. With the continuous development of control-forwarding separation technology and network function simulation technology, the characteristics of security protection automation, virtualization and dynamic flexibility make cloud computing develop healthily and orderly. Although the advantages of cloud computing are obvious, it also brings great challenges to information security protection. Relevant departments need to work out scientific and comprehensive protection measures from the influencing factors of information security, so as to improve information security.

References

[1] Liu Chuan, Li Zhiwei, Shen Weikang. Power data center security analysis and protection strategy based on cloud computing and SDN. Electronic Design Engineering, vol. 24, no. 9, pp. 142-144+149, 2016.

[2] Wang Gang. Multi-region secure cloud computing architecture based on SDN technology. Information Security Research, vol. 1, no. 1, pp. 86-91, 2015.

[3] Huang Chende. Discussion on Data Security Technology of Power Information System Based on Cloud Computing. Science and Technology Innovation, vol. 17, no. 33, pp. 27-28, 2015.

[4] Anonymous. SDN-based cloud security application research review. Journal of Network and Information Security, vol. 3, no. 5, pp. 10-25, 2017.

[5] Pang Shuanglong, Chen Xiaodan, Zeng Desheng, Shao Cui. Research on SDN-based Data Center Network Architecture in Cloud Computing Environment. Electronic Technology, vol. 525, no. 8, pp. 39-41, 2020.

[6] Graded protection evaluation method based on cloud security service platform. Mobile Communications, vol. 41, no. 21, pp. 10-15, 2017.

[7] Xuan Lefei. Design and implementation of cyberspace security training platform. Science and Technology Vision, vol. 230, no. 8, pp. 46-47, 2018.

[8] Li Tao, Li Yue. Computer Information Security and Secrecy Technology Application and Research in Cloud Computing Environment. Network Security Technology and Application, vol. 7, no. 199, pp. 81+83, 2017.

[9] Wu Xiaoli. Research on Security Strategy of Information System Based on Cloud Computing. Network Security Technology and Application, vol. 214, no. 10, pp. 76+80, 2018.

[10] Samanthula B K, Elmehdwi Y, Howser G, et al. A secure data sharing and query processing framework via federation of cloud computing. Information Systems, vol. 48, no. 3, pp. 196-212, 2015.

[11] Ahmad M, Amin M B, Hussain S, et al. Health Fog: a novel framework for health and wellness applications. Journal of Supercomputing, vol. 72, no. 10, pp. 1-19, 2016.

[12] M'barek, El, Haloui, et al. Towards Services-Based Enterprise Architecture for Cloud Computing-Opened Information Systems. Journal of Computers, vol. 10, no. 3, pp. 195-202, 2015.

[13] Iorga M, Karmel A. Managing Risk in a Cloud Ecosystem. IEEE Cloud Computing, vol. 2, no. 6, pp. 51-57, 2015.

[14] Lei Yanshun. Analysis of Power Information System Security Technology under the Background of Cloud Computing. Communication World, vol. 26, no. 9, pp. 241-242, 2019.

[15] Batista BG, Ferreira C, Segura D, et al. A QoS-driven approach for cloud computing addressing attributes of performance and security. Future Generation Computer Systems, vol. 68, no. 3, pp. 260-274, 2017 .

Authorized licensed use limited to: Mukesh Patel School of Technology & Engineering. Downloaded on July 11,2023 at 05:51:40 UTC from IEEE Xplore. Restrictions apply.